(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 812 147**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **00 09479**

(51) Int Cl[7] : **H 04 L 9/16,** G 06 K 19/07, H 04 N 1/44, 7/16

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 19.07.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 25.01.02 Bulletin 02/04.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *INNOVATRON SA Société anonyme* — FR.

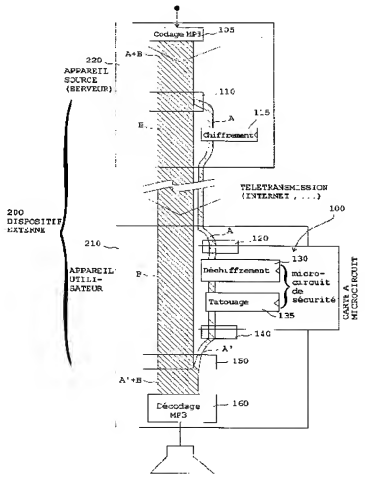
(72) **Inventeur(s) :** GRIEU FRANCOIS et MOLY JACQUES.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET BARDEHLE PAGENBERG ET PARTNER.

(54) PROCEDE DE TRAITEMENT D'UN FLUX D'INFORMATIONS PAR UN MICROCIRCUIT DE SECURITE, NOTAMMENT UN MICROCIRCUIT DE CARTE A PUCE.

(57) Le microcircuit (100) coopère avec un dispositif externe (200) apte à produire le flux d'informations sous forme de données numériques et à utiliser ce flux d'informations après traitement par le microcircuit. Le procédé comporte les étapes suivantes: a) par le dispositif externe, production du flux d'information; b) par le dispositif externe, séparation (110) du flux d'information incident (A+B) en deux fractions distinctes, avec une fraction mineure (A) et une fraction majeure (B), la fraction majeure présentant une taille et/ ou un débit d'information notablement supérieur à la fraction mineure; c) transmission (120) de la fraction mineure du dispositif externe au microcircuit; d) au sein du microcircuit, traitement sécuritaire (130, 135) de la fraction mineure; e) transmission (140) de la fraction mineure traitée (A') du microcircuit au dispositif externe; f) par le dispositif externe, recombinaison (150) de la fraction mineure traitée (A') avec la fraction majeure (B) de manière à produire un flux d'informations sortant (A'+B); g) par le dispositif externe, utilisation (160) du flux d'informations sortant (A'+B).



FR 2 812 147 - A1

L'invention concerne un procédé de traitement d'un flux d'informations numériques par un circuit de sécurité.

Elle concerne particulièrement le traitement d'informations représentatives de séquences reproductibles telles que séquences audio, vidéo, textuelles ou analogues.

On décrira l'invention principalement dans le cadre de séquences audio car il s'agit là de l'application la plus immédiate compte tenu des capacités actuelles des réseaux de diffusion ; toutefois, l'invention peut être transposée directement à l'acquisition d'autres types de séquences, notamment de données vidéo (images fixes ou images animées de télévision) ou de séquences textuelles. Elle s'applique de la même façon à l'acquisition de séquences formant fichiers de données de nature informatique, par exemple des données nécessaires au téléchargement d'un logiciel, ou pour permettre l'exécution par l'utilisateur d'un logiciel nécessitant un échange de données avec un site distant ; cette application se prête notamment au domaine des jeux électroniques téléchargés.

Il arrive fréquemment que l'on souhaite effectuer un ou plusieurs traitements sur un tel flux d'informations, traitement(s) opéré(s) dans un microcircuit de sécurité, par exemple le microcircuit d'une carte à puce, capable de stocker des informations dans une mémoire permanente et d'effectuer des calculs cryptographiques sur des informations (clefs) stockées dans ce microcircuit, et non lisibles de l'extérieur du microcircuit.

Les traitements que l'on souhaite effectuer sont en particulier :

- le déchiffrement et/ou le rechiffrement du flux ;
- le contrôle ou la génération d'un certificat ou signature électronique du flux ;
- le "tatouage", à savoir l'encodage ou décodage d'une information auxiliaire en filigrane du flux (c'est-à-dire superposant au flux une information imperceptible aux sens humains, mais que l'on peut détecter par des moyens appropriés) ; de tels systèmes sont par exemple décrits dans le US-A-5 687 191 (Solana Technology Development Corp.) ;
- l'extraction ou ajout d'informations au flux par démultiplexage ou multiplexage ;
- toutes opérations habituellement effectuée dans un microcircuit de sécurité, en particulier contrôles de toute nature, comptabilisation, paie-

ment, stockage.

L'intérêt de réaliser ces opérations dans un microcircuit de sécurité est en général de cacher une partie des informations utilisées dans le traitement, et/ou de garantir que tel ou tel traitement est bien effectué selon des règles imposées.

Ainsi, dans un exemple d'application que l'on exposera plus en détail par la suite, on souhaite qu'un flux de musique, numérisé et comprimé selon ISO/IEC 11172-3, soit chiffré, transmis à l'identique à plusieurs destinataires, déchiffré et tatoué par une information d'identification issue du microcircuit confié à chaque utilisateur. L'intérêt d'effectuer les opérations de déchiffrement et de tatouage dans un microcircuit de sécurité, plutôt que dans un micro-ordinateur par exemple, est que l'on est ainsi assuré que le flux d'information déchiffré et non tatoué n'est pas accessible, pas plus bien sûr que la clé de déchiffrement, ni celle servant à encoder le tatouage. Le besoin de tels traitements ressort notamment du WO-A-00/11866 pour *"Dispositif sécurisé décodeur d'informations chiffrées et comprimées"* (Innovatron SA), qui décrit une mise en œuvre particulièrement avantageuse du déchiffrement et de la décompression des signaux au moyen d'une carte à microcircuit.

On peut aussi considérer le problème consistant à extraire d'un flux audio ou vidéo des informations relatives à la gestion de droits d'exploitation, telles qu'identification du dispositif récepteur autorisé, nombre de copies autorisées, prix, et à effectuer des opérations telles que contrôle de l'identification et/ou des droits de copie, décrémentation du nombre de copies autorisées, paiement, tatouage du nombre de copies restant et/ou de l'identifiant du dispositif récepteur autorisé pour l'information résultante. Le besoin de tels traitements est apparent dans le US-A-5 892 900 (Intertrust Technologies Corp.).

Une réalisation selon les techniques courantes consisterait à transférer l'information au microcircuit, y réaliser les traitements et restituer l'information traitée. Elle se heurte à deux limitations pratiques :

- la vitesse de transmission des lecteurs de microcircuit existants : ceux-ci communiquent habituellement avec un débit de 9,6 kbit/s, et le débit utile est encore plus faible, de l'ordre de 5 kbit/s, alors que, dans un exemple de musique comprimée à 128 kbit/s, il faudrait un débit bien

plus élevé, de 256 kbit/s (le facteur 2 provenant du double flux entrant et sortant), pour traiter l'information à la vitesse de l'écoute.

- la capacité de traitement (déchiffrement et tatouage) du microcircuit est limitée.

L'un des buts de l'invention est de pallier cette difficulté de mise en œuvre pratique, par un moyen permettant de réduire la quantité d'informations échangées avec le microcircuit sans pour autant compromettre le caractère sécuritaire des traitements effectués dans le microcircuit – notamment sans accroître le risque de fraude.

Essentiellement, l'invention propose de sélectionner une petite fraction de l'information (typiquement moins de 20 % et par exemple entre 5 % et 1 %, voire moins de 1 %) qui sera extraite du flux total pour transmission et traitement par le microcircuit, puis de la recombiner avec la partie non traitée du flux. La fraction du flux extraite pour traitement dans la carte sera choisie de manière que sa présence soit importante, voire essentielle, pour la bonne réalisation des fonctions voulues d'exploitation de l'ensemble de l'information. Par exemple, dans le cas d'un flux de musique numérisée, en l'absence d'un traitement sécuritaire correct par la carte, des passages de la musique manqueraient périodiquement, ou seraient périodiquement déformés, rendant la reproduction de la musique inacceptable.

De cette manière, il est possible d'effectuer des traitements relativement complexes (déchiffrement, tatouage, calcul de clé, etc.) avec des cartes à microcircuit et des lecteurs traditionnels, dont la capacité de traitement serait largement insuffisante pour permettre un traitement de l'ensemble du flux, ce qui rend possible la mise en œuvre de ces traitements qui seraient autrement exclus.

Plus précisément, l'invention vise un procédé de traitement d'un flux d'informations par un microcircuit de sécurité, notamment un microcircuit de carte à puce, ce microcircuit coopérant avec un dispositif externe apte à produire le flux d'informations sous forme de données numériques et à utiliser ce flux d'informations après traitement par le microcircuit, caractérisé par les étapes suivantes :

a) par le dispositif externe, production du flux d'information,

b) par le dispositif externe, séparation du flux d'information incident en

deux fractions distinctes, avec une fraction mineure et une fraction majeure, la fraction majeure présentant une taille et/ou un débit d'information notablement supérieur à la fraction mineure,

c) transmission de la fraction mineure du dispositif externe au microcircuit,

d) au sein du microcircuit, traitement sécuritaire de la fraction mineure,

e) transmission de la fraction mineure traitée du microcircuit au dispositif externe,

f) par le dispositif externe, recombinaison de la fraction mineure traitée avec la fraction majeure de manière à produire un flux d'informations sortant,

g) par le dispositif externe, utilisation du flux d'informations sortant.

Selon diverses mises en œuvre subsidiaires avantageuses :

- le traitement sécuritaire de l'étape d) est un traitement du groupe comprenant : déchiffrement ou chiffrement du flux ; contrôle ou génération d'un certificat ou signature électronique du flux ; encodage ou décodage d'une information auxiliaire tatouée dans le flux ; extraction ou ajout d'une information au flux par démultiplexage ou multiplexage ; contrôle de validité du flux ; gestion de droits d'exploitation des informations du flux ; combinaison de deux ou plusieurs des traitements précédents ;
- le dispositif externe comporte un appareil source et un appareil utilisateur distincts, le microcircuit coopérant avec l'appareil utilisateur, les étapes a) et b) sont mises en œuvre dans l'appareil source, et l'étape f) est mise en œuvre dans l'appareil utilisateur ;
- après l'étape b) de séparation et avant l'étape c) de transmission, il est prévu une étape de traitement, notamment de chiffrement, de la fraction mineure (A) par le dispositif externe, l'étape d) de traitement sécuritaire mise en œuvre au sein du microcircuit étant une étape d'un traitement symétrique, notamment une étape de déchiffrement ;
- le traitement sécuritaire de l'étape d) inclut un transcodage de clé, comportant un déchiffrement avec une première clé puis un rechiffrement avec une seconde clé ;
- la séparation de l'étape b) comporte une séparation temporelle, opérée par découpage du flux incident en intervalles de temps, et/ou une séparation fonction du contenu informationnel des données composant

le flux incident, opérée par extraction de champs de données de nature prédéterminée ;

- la séparation de l'étape b) et/ou le traitement sécuritaire est fonction de paramètres influant la perceptibilité de la séparation et/ou du traitement et sélectionnés afin d'en réduire la perceptibilité ;
- le traitement sécuritaire de l'étape d) comprend également la production d'une clé apte à permettre le déchiffrement de la fraction majeure par le dispositif externe ;
- la taille et/ou le débit d'informations de la fraction mineure sont inférieurs à 20 % du flux total, de préférence compris entre 5 % et 1 % du flux total, avantageusement inférieurs à 1 % du flux total.

◊

On va maintenant décrire un exemple de mise en œuvre de l'invention, en référence aux dessins annexés.

La figure 1 illustre de façon schématique les différentes étapes du procédé de l'invention.

La figure 2 illustre, sous forme de blocs fonctionnels, différents éléments impliqués dans une mise en œuvre particulière du procédé de l'invention.

◊

La mise en œuvre de l'invention implique, comme illustré figure 1, au moins deux organes distincts, à savoir un microcircuit de sécurité 100 et, d'autre part, un ensemble que l'on appellera "dispositif externe" 200, correspondant à l'environnement extérieur, non sécurisé ou partiellement sécurisé, de ce microcircuit 100.

Le microcircuit de sécurité peut être par exemple un *ST16SF48* de STMicroelectronics, encarté dans une carte selon ISO/IEC 7816-1 à -3 et relié à son environnement par un lecteur de carte à microcircuit conforme à ces standards ou de manière équivalente (aussi bien amovible que permanente), par exemple à travers un bus de type USB.

Dans l'exemple que l'on va décrire, le dispositif externe 200 est constitué d'un "appareil utilisateur" 210 et d'un "appareil source" 220 reliés entre

eux par une voie de communication telle qu'une liaison Internet ou toute autre voie de télétransmission.

Cette mise en œuvre dans laquelle le dispositif externe 200 est constitué de deux organes distincts et distants 210 et 220 n'est cependant pas limitative, et l'invention s'applique aussi bien au traitement d'informations produites et utilisées par un seul et même appareil.

Dans l'exemple que l'on va décrire, l'appareil utilisateur 210 peut notamment être un dispositif de type "tuner Internet" tel que décrit dans les WO-A-00/11867 pour *"Procédé de délivrance certifiée d'une séquence audio, vidéo ou textuelle"* (Innovatron SA) et WO-A-00/11868 pour *"Procédé de délivrance et de paiement d'une séquence audio, vidéo ou textuelle"* (Innovatron SA). Ces demandes décrivent des moyens permettant d'acquérir pour écoute des séquences audio, typiquement des œuvres musicales telles que des morceaux de musique ou des plages individuelles d'un enregistrement, convenablement sélectionnées par l'usager. Les morceaux de musique sont téléchargés sous forme de paquets de données numériques éventuellement signées, chiffrées et comprimées, et transmis depuis un site central (appareil source) à l'appareil utilisateur.

L'appareil utilisateur 210 comporte à cet effet des moyens, intégrés ou séparés, de reproduction sonore, divers circuits de décompression, décryptage, paiement, contrôle d'accès, etc., notamment des circuits mettant en œuvre une ou plusieurs cartes à microcircuit, ainsi que des moyens de connexion à un site distant (site central ou bien délocalisé en plusieurs sites). Le téléchargement est typiquement réalisé via Internet, c'est-à-dire par les réseaux mondiaux interconnectés reliant des sites et des utilisateurs par des routages variables et multiples pour la transmission de données sous forme numérique.

L'appareil source 220 est par un exemple un micro-ordinateur configuré en serveur Internet, ou même un simple support de stockage tel que cédérom ou DVD-ROM.

L'information originelle destinée à être traitée est tout d'abord numérisée et avantageusement comprimée et codée, par exemple, dans le cas de la musique, par un codage ISO/IEC 11172-3 *layer* 3 ('MP3') (étape 105).

De façon caractéristique de l'invention, le flux résultant 110 est ensuite séparé en deux fractions distinctes, une fraction mineure A (représentant

par exemple entre 5 % et 1 % en volume du flux global), et une fraction majeure B (représentant donc respectivement entre 95 % et 99 % du flux global A+B). Le flux A est défini de manière à contenir des informations nécessaires, voire indispensables, à une exploitation correcte du flux global A+B.

La séparation de l'étape 110 peut être opérée de différentes manières, qui peuvent au surplus être combinées entre elles.

Dans une première variante, la séparation est une séparation temporelle. L'information est alors divisée en intervalles de temps correspondant au temps de transmission ou, pour un flux audio ou vidéo, au temps de restitution aux sens humains. Une fraction prédéterminée de ces intervalles constitue A, et le reste B. Cette sélection temporelle trouve sa justification dans le fait qu'un message audio ou vidéo amputé périodiquement d'une partie significative de son contenu devient inutilisable. Par exemple, le flux A retient des intervalles de 0,2 seconde toutes les 4 secondes. Comme le flux d'information audio ou vidéo est fréquemment, par son codage même, structuré en trames représentant des intervalles de temps distincts (dénommés "*frames*" dans ISO/IEC 11172-3), ce découpage temporel revient alors à retenir pour le flux A une fraction des trames : par exemple, si une trame dure 0,025 s, alors le flux A retiendra 8 trames sur 160. Ceci est un exemple d'un cas où il peut être avantageux que la fraction mineur représente entre 5 % et 1 % du flux total A+B, cette fraction étant suffisamment importante pour assurer une dégradation inacceptable du contenu si elle n'est pas reproduite, tout en réduisant fortement la charge du microcircuit.

Dans une seconde variante, la séparation est une séparation par nature d'informations.

Le flux d'information est divisé par un facteur 200, ce qui permet de réduire la charge du microcircuit à moins de 1 % du flux total A + B tout en garantissant la sécurité, en sélectionnant préférentiellement pour le flux A les informations de nature prédéterminée qui sont les plus importantes pour l'intelligibilité du flux par les sens humains et/ou celles adaptées au traitement considéré et/ou celles nécessaires pour l'exploitation de l'ensemble de l'information et/ou dont la reconstitution en cas d'altération est la plus difficile. Par exemple, selon ISO/IEC 11172-3 chaque trame est

découpée en de nombreux champs, et pour rendre tout à fait inutilisable un flux audio ISO/IEC 11172-3 *layer III* il suffit de chiffrer le champs *Huffmancodebits* (voir §2.4.1.7 de la norme, page 19), ou encore les seuls bits *signx* et *signy*, ou encore un nombre prédéterminé de bits *signx* et *signy* choisis comme étant ceux de certaines valeurs de l'indice *I*, par exemple comme un nombre prédéterminé de celles pour lesquelles |*x*| et |*y*| sont les plus grandes, éventuellement en se restreignant à un intervalle de *I*.

Dans le cas d'un traitement consistant en un tatouage, on retiendra dans le flux A les informations codant les grandeurs qui, compte tenu du système, sont à modifier pour l'inscription du filigrane ; il s'agira par exemple des informations dans une bande de fréquence prédéterminée et/ou celle dont l'amplitude est la plus grande et/ou la plus constante et/ou dans la limite d'un plafond de quantité ou de débit d'information prédéterminé limitant la quantité d'information incluse dans le flux A.

De plus, les deux variantes que l'on vient de décrire peuvent être combinées entre elles, de diverses façons. Ainsi :

- on peut simplement ne retenir qu'une fraction des informations ("sélection par nature" ci-dessus) d'une fraction temporelle ("sélection temporelle" ci-dessus) du flux, ce qui multiple les effets de réduction du flux A.
- on peut aussi effectuer une sélection temporelle selon l'adéquation au traitement à effectuer : on examine les intervalles de temps du flux pour déterminer leur adéquation au traitement à effectuer (tel que tatouage) et l'on sélectionne préférentiellement ceux des intervalles du flux qui sont les plus aptes à subir le traitement (avec une dégradation minimale de la qualité perçue et/ou une meilleure capacité de codage, ces paramètres variant considérablement selon les intervalles de temps), dans la limite d'un plafond prédéterminé limitant la quantité d'information incluse dans le flux A.

La combinaison des deux techniques de sélection peut permettre d'avoir pour A une fraction encore plus faible que 1% de l'information totale, ce qui permet l'utilisation de microcircuits et de lecteurs de microcircuit actuellement disponibles, sans attendre des progrès futurs de leurs performances, tout en maintenant le niveau de sécurité requis pour le traitement

(déchiffrement et tatouage).

Avant transmission à l'appareil utilisateur, il est souvent utile de prévoir, au niveau du serveur, une étape supplémentaire 115 de traitement du flux A, par exemple une étape de chiffrement au moyen d'une clé secrète K et d'un algorithme symétrique.

Les flux A et B ainsi préparés par le serveur source 220 sont alors transmis à l'appareil utilisateur 210, qui reçoit donc concurremment ces deux flux A et B, par exemple multiplexés pour permettre leur transmission sur un canal commun.

À réception, le flux A est isolé et transmis (en 120) au microcircuit de sécurité 100. Celui-ci déchiffre alors le flux A (étape 130) au moyen de la clé K qu'il contient ou qu'il est capable de recalculer. Si l'on souhaite en outre tatouer la musique avant de la restituer, le microcircuit opère ensuite un tatouage (étape 135) par inscription en filigrane dans le flux A d'un identifiant propre au microcircuit (ou d'un autre identifiant spécifique à la carte et/ou à l'utilisateur)

Le flux résultant A' est transmis en retour (en 140) à l'appareil utilisateur.

Ce dernier combine les flux A' et B (étape 150) et transforme le tout en un signal sonore reproductible, par exemple par le décodage ISO/IEC 11172-3 *layer* 3 ('MP3') de l'étape 160.

Le procédé que l'on vient de décrire peut faire l'objet de différentes adaptations ou améliorations.

Ainsi, dans le cas d'une sélection temporelle, il peut être utile à une étape supplémentaire (située après le chiffrement 115) de réordonner les segments de manière à permettre une restitution la plus aisée possible, sans attente au début et avec un minimum de mémoire dans le dispositif de restitution. Prenons l'exemple de trames numérotées consécutivement de 01 à 30, les trames multiples de 10 faisant partie du flux A. Il sera utile à cette étape supplémentaire de réordonner le flux dans l'ordre :

10 01 02 03 04 05 06 07 08 09 20 11 12 13 14 15 16 17 18 19 30 21 22 23 24 25 26 27 28 29.

De la sorte, la restitution sonore des trames n° 01 à 09 pourra se faire pendant que la trame n° 10 sera transmise et traitée par le microcircuit (étapes 120 à 140), opérations relativement longues.

De même les trames n° 20 et 30 seront traitées pendant la restitution des

trames n° 11 à 19 et 20 à 29.

Un autre perfectionnement consiste à combiner la technique de l'invention avec une technique différente, en elle-même connue et utilisée notamment en télévision à péage, visant à réduire par un autre moyen la quantité d'informations manipulées par le microcircuit (mais dans le seul cas d'un traitement de déchiffrement conditionnel).

Dans cette technique connue :

- on choisit une clé K (éventuellement variable dans le temps) ;
- on chiffre le flux audio ou vidéo F avec cette clé K, produisant F' ;
- on chiffre la clé K avec une autre clé, produisant K' ;
- on combine le flux F' et la clé K' par multiplexage ;
- on transmet l'ensemble à un décodeur ;
- le décodeur sépare F' et la clé K' ;
- le décodeur transmet la clé K' au microcircuit ;
- le microcircuit déchiffre la clé K', produisant K ;
- le microcircuit transmet la clé K au décodeur ;
- le décodeur déchiffre le flux F', produisant le flux F d'origine.

On notera que dans cette technique connue l'information utile F (audio ou vidéo) ne transite pas dans le microcircuit, alors qu'elle le fera en partie dans le système objet de la présente invention (avec l'avantage caractéristique de permettre dans le microcircuit même un traitement arbitraire, tel qu'un tatouage, de l'information utile).

Ainsi, l'information restituée dans cette technique connue est identique à l'information d'origine, alors que l'invention permet son traitement partiel dans le microcircuit. En pratique, la combinaison de l'information issue du microcircuit et du flux principal se fait par déchiffrement dans la technique de la télévision à péage, alors qu'elle se fait par ajout ou multiplexage dans une forme de l'invention.

On peut utilement combiner cette technique connue avec celle de la présente invention, en particulier pour déchiffrer le flux B. On peut par exemple ajouter au système précédent les étapes suivantes :

- au serveur source, en amont de l'étape 115 de chiffrement :
  - on choisit une clé aléatoire KB,
  - on chiffre le flux B avec KB, et
  - on multiplexe la valeur de KB avec A ;

- à l'étape 115, on chiffre KB et A ensemble avec K (on pourrait prévoir une étape séparée) ;
- on transmet KB' et A chiffrés à l'appareil utilisateur (on pourrait prévoir une étape séparée) ;
- à l'étape 120, on transmet KB' et A chiffrés ensemble au microcircuit de sécurité (on pourrait prévoir une étape séparée) ;
- à l'étape 130, on déchiffre KB et A (on pourrait prévoir une étape séparée) ;
- à l'étape 140, on transmet KB et A' à l'appareil utilisateur (on pourrait prévoir une étape séparée) ;
- en amont de l'étape 150 de recombinaison :
  - on extrait la clé KB du flux A', de manière symétrique à celle du multiplexage par le serveur source ; et
  - on déchiffre le flux B avec KB, de manière symétrique à celle du chiffrement par le serveur source.

On remarquera que, si l'on combine le chiffrement du flux B et la technique de réordonnancement des trames exposée plus haut, la clé KB chiffrant les trames n° 11 à 19 doit être dans le bloc n° 10, et non dans le bloc n° 20.

Il peut être utile de prévoir que le microcircuit déchiffre la clé K', donnant K, et la rechiffre d'une manière différente, donnant K''.

Par ailleurs, en supplément des clés de chiffrement, des informations liées au flux (telles que droits de reproduction) peuvent être extraites du flux et traitées par le microcircuit.

Ainsi, le traitement 30 peut comprendre :

- déchiffrement avec une première clé, et
- rechiffrement avec une deuxième clé.

Ce transcodage de clef autorise par exemple le déchiffrement dans le dispositif utilisateur d'un flux en provenance du serveur, notamment après paiement, le rechiffrement limitant sa réutilisation ultérieure à un autre appareil spécifiquement désigné par la clé de rechargement (par exemple un baladeur particulier).

La figure 2 illustre, sous forme de blocs fonctionnels, différents éléments impliqués dans une mise en oeuvre particulière du procédé que l'on vient de décrire.

Cette configuration est destinée à permettre la diffusion d'un contenu multimédia (audio, vidéo, jeux, etc.) de l'appareil source (serveur) 220, où ce contenu multimédia est préparé et rendu disponible de la manière que l'on va décrire, vers l'appareil destinataire 210 d'un client :

- en s'assurant que le contenu ne sera disponible que pour les clients qui se seront acquitté d'un droit de visualisation,
- en permettant également de garantir les paiements et faire respecter les règles définies par les ayants-droit (par exemple un nombre limité de visualisations autorisées),
- en procurant enfin une certaine traçabilité permettant, en cas de fraude, de pouvoir remonter au serveur et/ou déterminer l'acheteur à l'origine de la copie.

L'appareil destinataire 210 du client est un ensemble matériel et logiciel constitué autour d'un équipement de type connu tel que micro-ordinateur, décodeur de TV numérique (notamment du type "*set top box*"), ou encore téléphone portable apte à échanger des données numériques conformément aux normes GSM, WAP, GPRS, UMTS ou autres.

A cet équipement sont associés :

- un logiciel d'application client 211,
- le microcircuit 100,
- éventuellement un moyen de stockage de masse 213 tel que disque dur, mémoire flash, etc.,
- un périphérique 214 de restitution du contenu multimédia, par exemple moniteur de télévision, amplificateur audio, assistant numérique personnel, graveur de disque compact, etc.

Le contenu multimédia est tout d'abord préparé au niveau du serveur source 220 de la manière suivante.

Ce contenu, désigné "contenu de valeur" sur la figure 2, est accompagné de "règles d'usage" qui définissent les restrictions d'utilisation, le nombre de copies utilisées, la durée de péremption, etc. Ces règles peuvent être éventuellement des règles non spécifiques, appliquées par défaut lorsque le contenu de valeur n'est associé à aucune règle propre.

Le contenu multimédia peut également comprendre des informations, désignées "contenu sans valeur", ne nécessitant pas de mesures de protection particulières, par exemple biographie de l'interprète, paroles d'une

chanson, jaquette de présentation, etc.

Les règles d'usage sont incorporées au contenu de valeur, par exemple et de manière en elle-même connue par tatouage, puis l'ensemble est découpé en blocs, signé et chiffré, pour produire enfin :

- d'une part le contenu de valeur, sous forme de blocs signés et chiffrés, ce contenu de valeur incorporant les règles d'usage,
- d'autre part, un "titre d'accès" associé, qui permettra de contrôler l'accès au contenu multimédia et sa restitution par l'appareil destinataire de la manière que l'on indiquera plus bas (le terme "titre" étant entendu dans son acception juridique (comme dans "titre de transport" ou "titre de créance"), c'est-à-dire comme certificat constatant un acte juridique ou matériel susceptible de produire des effets – ici l'autorisation de reproduction ou de duplication du contenu),
- et éventuellement le contenu sans valeur, simplement découpé en blocs.

Cet ensemble de données est stocké par le serveur 220.

La transaction serveur-client s'effectue de manière sécurisée entre le serveur et le microcircuit 100 selon des techniques en elles-mêmes connues, le logiciel d'application client 211 servant de passerelle entre le serveur et le microcircuit.

Pour assurer la sécurisation, le microcircuit et le serveur échangent des certificats, avec par exemple :

- un premier certificat, du microcircuit vers le serveur, pour certifier que l'utilisateur du microcircuit a bien acquitté le prix correspondant au contenu de valeur précisément identifié, et
- un second certificat, du serveur vers le microcircuit, pour transmettre à ce dernier le titre d'accès, ce titre pouvant éventuellement contenir une clef de décryptage.

Ces certificats sont signés et cryptés à l'aide de clefs conservées d'une manière sécurisée dans le microcircuit et dans le serveur. Les transactions entre ces deux organes sont ainsi sécurisées, même au travers d'un canal non sûr (réseau téléphonique, réseau câblé, Internet, etc.).

Une fois ces opérations effectuées, l'ensemble des blocs du contenu demandé (contenu de valeur et contenu sans valeur) est transmis à l'appareil destinataire.

Toute opération en provenance ou à destination d'un périphérique, y compris le périphérique de restitution local 214, ne peut se faire qu'au travers du microcircuit 100, ce dernier ne répondant à cet effet qu'à des commandes dûment signées et authentifiées.

Après préparation et transfert du contenu multimédia, l'appareil destinataire dispose du contenu de valeur, crypté avec les règles qui doivent en régir l'accès, et éventuellement d'un ensemble d'informations non secrètes (contenu sans valeur, qui peut être affiché par le périphérique de restitution 214, ou bien simplement ignoré).

On va tout d'abord décrire une mise en œuvre dans laquelle le contenu de valeur est restitué en "*streaming*" c'est-à-dire restitué sous une forme intelligible aux sens humains au fur et à mesure de sa réception, sensiblement à la vitesse à laquelle il est transmis, sans stockage permanent dans le dispositif utilisateur (qui ne stocke qu'une quantité limitée d'informations, par exemple correspondant à une seconde de restitution pour amortir les fluctuations de courte durée du moyen de transmission).

Les blocs sont transmis à l'appareil destinataire qui émet une commande de déchiffrement au microcircuit en lui passant le bloc. Le microcircuit n'accepte bien entendu ces commandes que si elles ont été convenablement signées et authentifiées. Il calcule la signature du bloc et vérifie les conditions d'accès, en particulier le fait que l'utilisateur a bien le droit de recevoir le contenu en "streaming" et qu'il s'est bien acquitté du paiement des droits de lecture ; il utilise pour cela le titre d'accès qu'il a reçu suite au paiement, avec les règles qui ont été tatouées et/ou incluses dans le contenu de valeur.

Conformément à la présente invention, le contenu de valeur incorporant les règles est divisé (étape 110 de la figure 1) en deux flux distincts A et B de façon pertinente, c'est-à-dire de manière à rendre inexploitable le flux B seul, ou le flux A+B, sans que A n'ait été ultérieurement traité par le microcircuit.

Le flux B (fraction majeure, typiquement 95 ou 99 % en volume du flux total A+B) est chiffré avec une première clé, ou éventuellement laissé en clair.

En revanche, le flux A, qui doit être traité avec le maximum de sécurité, est chiffré (étape 115 de la figure 1), de même que les règles et la pre-

mière clé précitées, de façon à n'être déchiffrable ultérieurement que par le microcircuit de sécurité.

De façon caractéristique de l'invention, seul le flux A est transmis au microcircuit, ou il sera déchiffré et tatoué (étapes 130 et 135 de la figure 1).

Éventuellement, le microcircuit peut également rechiffrer le flux A avec une clé associée au périphérique de restitution particulier 214.

Par ailleurs, le microcircuit restitue et transmet à l'appareil utilisateur la première clé précitée, c'est-à-dire celle qui permet le déchiffrement du flux B au cas où celui-ci n'a pas été transmis en clair.

Ce déchiffrement du flux B est opéré à l'extérieur du microcircuit, dont les capacités mémoire et de traitement seraient insuffisantes pour assurer cette opération en temps réel.

Le périphérique 214 peut alors restituer le contenu multimédia.

Lorsque le "streaming" n'est pas possible ou pas souhaité, le contenu est simplement téléchargé, c'est-à-dire que les informations correspondantes sont stockées intégralement et de manière permanente dans le moyen de stockage 213 pour restitution ultérieure.

La procédure décrite ci-dessus est alors adaptée de la manière suivante.

Le logiciel d'application client 211 sert de passerelle entre le serveur source 220, le microcircuit 100 et le périphérique de restitution 214. Le périphérique 214 et le microcircuit 100 peuvent éventuellement s'identifier, par exemple par échange de certificats contenant des données aléatoires. Ils peuvent également échanger des clefs entre eux pour communiquer de manière chiffrée.

Le logiciel d'application client 211 transmet des commandes signées et cryptées au microcircuit 100 en y attachant les blocs. Bien entendu, le microcircuit n'accepte ces commandes que si elles ont été convenablement signées et authentifiées.

Le microcircuit calcule la signature du bloc et vérifie les conditions d'accès, en particulier le fait que l'utilisateur a bien le droit de copier le contenu et qu'il s'est bien acquitté du paiement des droits de lecture. Il utilise pour cela le titre d'accès qu'il a reçu suite au paiement, avec les règles qui ont été tatouées ou incluses dans le contenu de valeur.

Si toutes les conditions sont bien respectées, le microcircuit déchiffre le flux A, le rechiffre éventuellement avec une clef associée au périphérique

de restitution et transmet ce contenu au périphérique 213, qui peut alors stocker ce contenu multimédia, à partir duquel la restitution sera effectuée ultérieurement.

Dans le cas où l'utilisateur tente de transférer le contenu téléchargé vers un autre moyen de stockage, le microcircuit 100 n'autorisera la recopie que pour un contenu dont il a les droits d'accès, à moins qu'il ne s'agisse d'un contenu marqué "libre de droits". Dans le cas où les droits sont présents, il n'y a pas en principe de recopie, puisque le contenu est déjà stocké sur le moyen de stockage de l'appareil de l'utilisateur.

REVENDICATIONS

1. Un procédé de traitement d'un flux d'informations par un microcircuit de sécurité (100), notamment un microcircuit de carte à puce, ce microcircuit coopérant avec un dispositif externe (200) apte à produire le flux d'informations sous forme de données numériques et à utiliser ce flux d'informations après traitement par le microcircuit,
procédé caractérisé par les étapes suivantes :

a) par le dispositif externe, production du flux d'information,
b) par le dispositif externe, séparation (110) du flux d'information incident (A+B) en deux fractions distinctes, avec une fraction mineure (A) et une fraction majeure (B), la fraction majeure présentant une taille et/ou un débit d'information notablement supérieur à la fraction mineure,
c) transmission (120) de la fraction mineure du dispositif externe au microcircuit,
d) au sein du microcircuit, traitement sécuritaire (130, 135) de la fraction mineure,
e) transmission (140) de la fraction mineure traitée (A') du microcircuit au dispositif externe,
f) par le dispositif externe, recombinaison (150) de la fraction mineure traitée (A') avec la fraction majeure (B) de manière à produire un flux d'informations sortant (A'+B),
g) par le dispositif externe, utilisation (160) du flux d'informations sortant (A'+B).

2. Le procédé de la revendication 1, dans lequel le traitement sécuritaire de l'étape d) est un traitement du groupe comprenant : déchiffrement ou chiffrement du flux ; contrôle ou génération d'un certificat ou signature électronique du flux ; encodage ou décodage d'une information auxiliaire tatouée dans le flux ; extraction ou ajout d'une information au flux par démultiplexage ou multiplexage ; contrôle de validité du flux ; gestion de droits d'exploitation des informations du flux ; et combinaison de deux ou plusieurs des traitements précédents.

3. Le procédé de la revendication 1 ou 2, dans lequel :
- le dispositif externe comporte un appareil source (220) et un appareil utilisateur (210) distincts, le microcircuit (100) coopérant avec l'appareil utilisateur (210) ;
- les étapes a) et b) sont mises en œuvre dans l'appareil source ; et
- l'étape f) est mise en œuvre dans l'appareil utilisateur.

4. Le procédé de l'une des revendications 1 à 3, dans lequel, après l'étape b) de séparation et avant l'étape c) de transmission, il est prévu une étape (115) de traitement, notamment de chiffrement, de la fraction mineure (A) par le dispositif externe, l'étape d) de traitement sécuritaire mise en œuvre au sein du microcircuit étant une étape d'un traitement symétrique, notamment une étape de déchiffrement (130).

5. Le procédé de la revendication 4, dans lequel le traitement sécuritaire de l'étape d) inclut un transcodage de clé, comportant un déchiffrement avec une première clé puis un rechiffrement avec une seconde clé.

6. Le procédé de l'une des revendications 1 à 5, dans lequel la séparation de l'étape b) comporte une séparation temporelle, opérée par découpage du flux incident en intervalles de temps.

7. Le procédé de l'une des revendications 1 à 6, dans lequel la séparation de l'étape b) comporte une séparation fonction du contenu informationnel des données composant le flux incident, opérée par extraction de champs de données de nature prédéterminée.

8. Le procédé de l'une des revendications 1 à 7, dans lequel la séparation de l'étape b) est une séparation à la fois temporelle et fonction du contenu informationnel des données composant le flux incident, opérée par découpage du flux incident en intervalles de temps et extraction de champs de données de nature prédéterminée.

9. Le procédé de l'une des revendications 1 à 8, dans lequel la séparation de l'étape b) et/ou le traitement sécuritaire (130, 135) est fonction de pa-

ramètres influant la perceptibilité de la séparation et/ou du traitement et sélectionnés afin d'en réduire la perceptibilité.

10. Le procédé de l'une des revendications 1 à 9, dans lequel le traitement sécuritaire de l'étape d) comprend également la production d'une clé apte à permettre le déchiffrement de la fraction majeure (B) par le dispositif externe.

11. Le procédé de l'une des revendications 1 à 10, dans lequel la taille et/ou le débit d'informations de la fraction mineure (A) sont inférieurs à 20 % du flux total (A+B).

12. Le procédé de la revendication 11, dans lequel la taille et/ou le débit d'informations de la fraction mineure (A) sont compris entre 5 % et 1 % du flux total (A+B).

13. Le procédé de la revendication 11, dans lequel la taille et/ou le débit d'informations de la fraction mineure (A) sont inférieurs à 1 % du flux total (A+B).

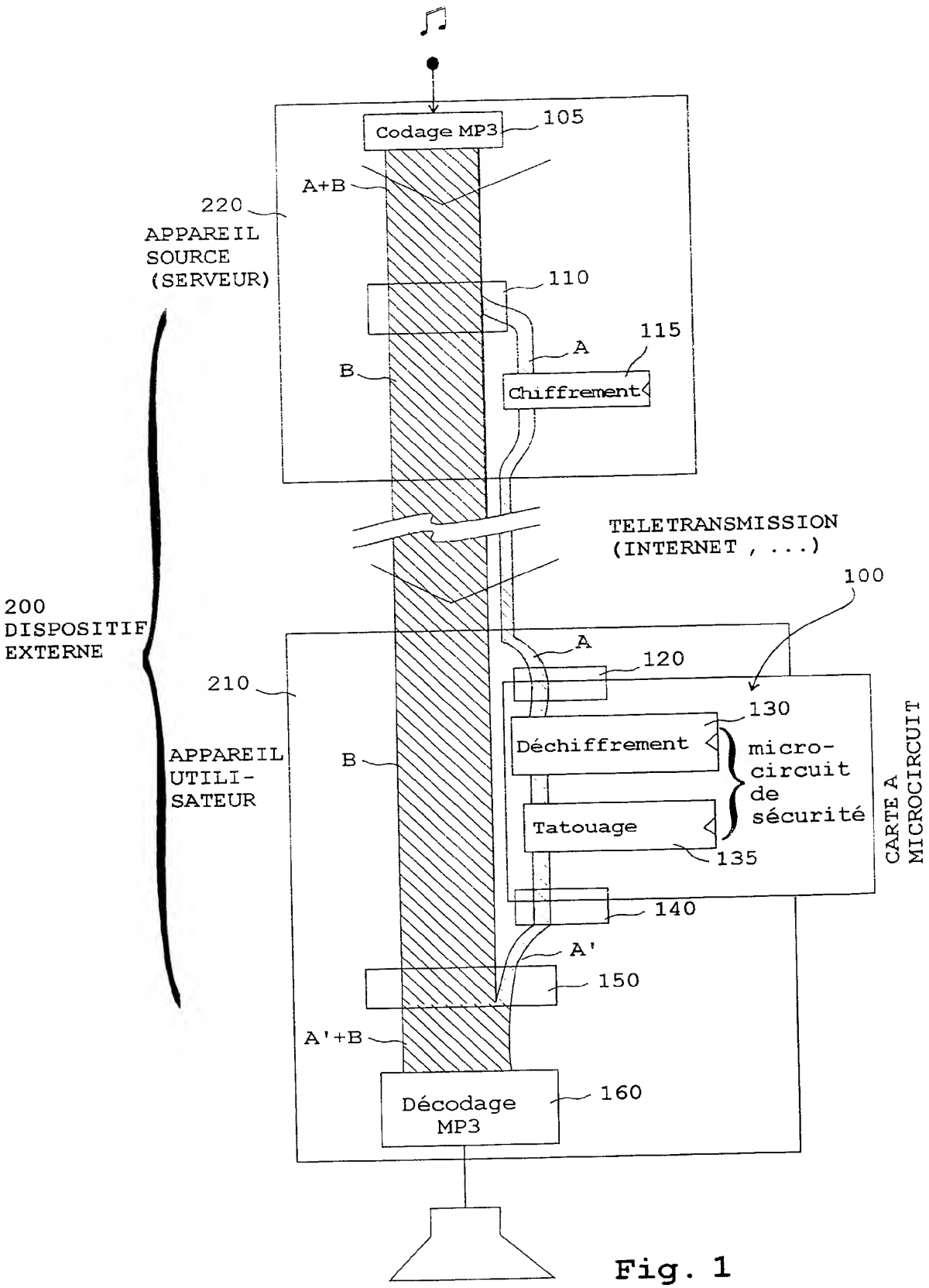

Codage MP3
105
A+B
220
APPAREIL SOURCE (SERVEUR)
110
115
A
B
Chiffrement
TELETRANSMISSION (INTERNET , ...)
100
200 DISPOSITIF EXTERNE
A
120
210
130
Déchiffrement
micro-circuit de sécurité
APPAREIL UTILI-SATEUR
B
Tatouage
135
CARTE A MICROCIRCUIT
140
A'
150
A'+B
Décodage MP3
160

Fig. 1

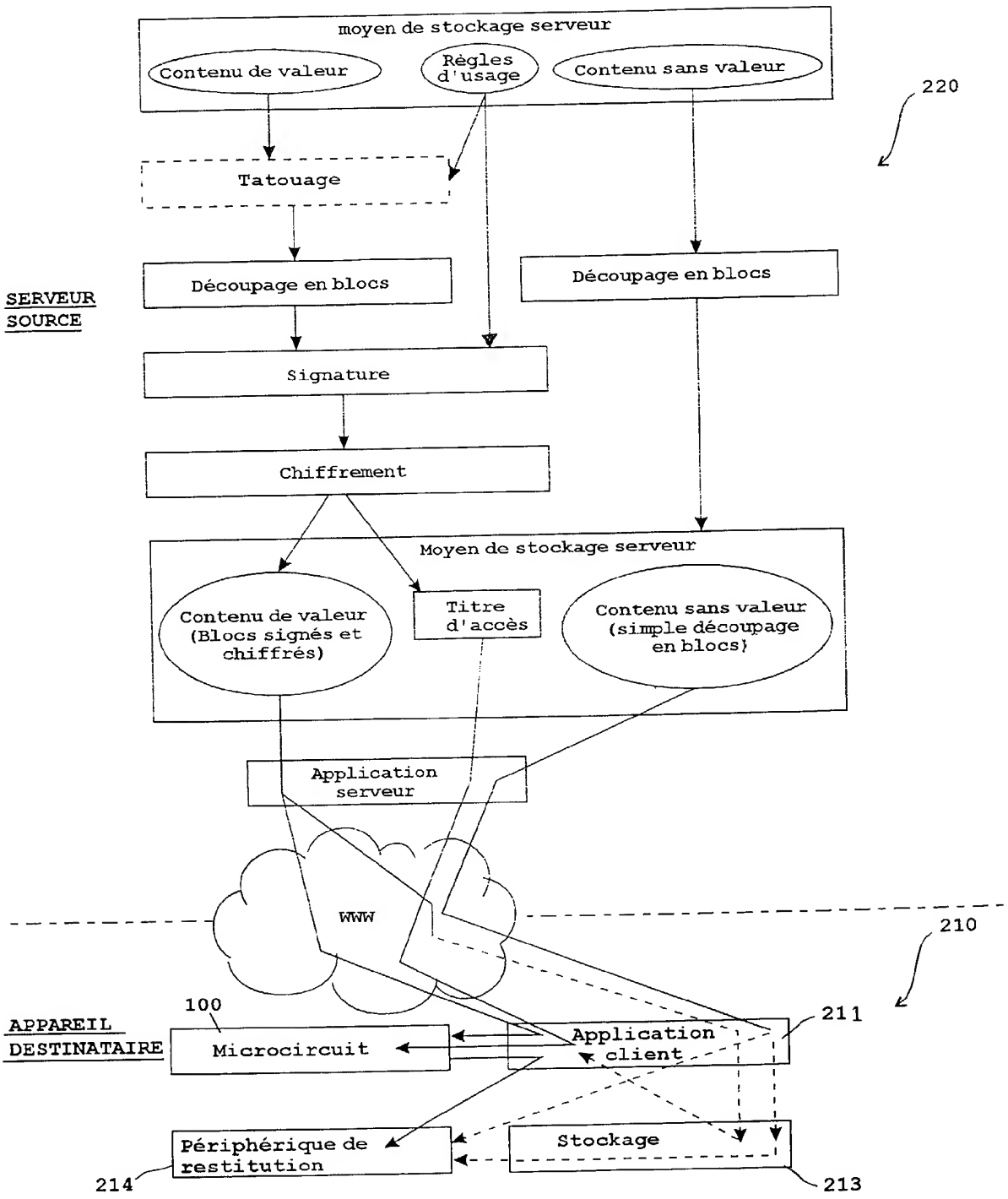

moyen de stockage serveur
Contenu de valeur
Règles d'usage
Contenu sans valeur
220
Tatouage
SERVEUR SOURCE
Découpage en blocs
Découpage en blocs
Signature
Chiffrement
Moyen de stockage serveur
Contenu de valeur (Blocs signés et chiffrés)
Titre d'accès
Contenu sans valeur (simple découpage en blocs)
Application serveur
WWW
210
100
APPAREIL DESTINATAIRE
Microcircuit
Application client
211
Périphérique de restitution
Stockage
214
213

Fig. 2

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2812147
N° d'enregistrement national

FA 592702
FR 0009479

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	WO 00 31964 A (ERICSSON TELEFON AB L M) 2 juin 2000 (2000-06-02) * page 9 * ---	1-4,6-13	H04L9/16 G06K19/07 H04N1/44 H04N7/16
A	KUNKELMANN T ; HORN U : "Video encryption based on data partitioning and scalable coding - a comparaison" INTERACTIVE DISTRIBUTED MULTIMEDIA SYSTEMS AND TELECOMMUNICATION SERVICES. 5TH INTERNATIONAL WORKSHOP, IDMS '98. PROCEEDINGS, PROCEEDINGS OF 5TH INTERNATIONAL WORKSHOP ON INTERACTIVE DISTRIBUTED MULTIMEDIA SYSTEMS AND TELECOMMUNICATION SERVICE,, 8 - 11 septembre 1998, pages 95-106, XP002165338 Oslo, Norway * le document en entier * ---	1,2,4-9, 11-13	
A	AGI I ; GONG L: "An empirical study of secure MPEG video transmissions" PROCEEDINGS OF THE SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEM SECURITY, PROCEEDINGS OF INTERNET SOCIETY SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEMS SECURITY, 22 - 23 février 1996, pages 137-144, XP002165339 San Diego, CA, USA * le document en entier * ---	1,2,4-9, 11-13	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) H04N
A	US 5 799 082 A (JANKY JAMES M ET AL) 25 août 1998 (1998-08-25) * colonne 11, ligne 36 - colonne 13, ligne 52 * --- -/--	1,2,4,7	

3

Date d'achèvement de la recherche	Examinateur
12 avril 2001	Marie-Julie, J-M

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2812147
N° d'enregistrement national

FA 592702
FR 0009479

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	KUNKELMANN T ; REINEMA R : "A scalable security architecture for multimedia communication standards " PROCEEDINGS IEEE INTERNATIONAL CONFERENCE ON MULTIMEDIA COMPUTING AND SYSTEMS '97 (CAT. NO.97TB100141), PROCEEDINGS OF IEEE INTERNATIONAL CONFERENCE ON MULTIMEDIA COMPUTING AND SYSTEMS, 3 - 6 juin 1997, pages 660-661, XP002165340 Ottawa, Ont., Canada * le document en entier * ---	1	
A	PATENT ABSTRACTS OF JAPAN vol. 1999, no. 04, 30 avril 1999 (1999-04-30) & JP 11 018070 A (MATSUSHITA ELECTRIC IND CO LTD), 22 janvier 1999 (1999-01-22) * abrégé * -----	1	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

Date d'achèvement de la recherche	Examinateur
12 avril 2001	Marie-Julie, J-M

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

3

EPO FORM 1503 12.99 (P04C14)